DOI: 10.16538/j.cnki.jsufe.2022.05.010

云计算环境下商业秘密保密措施的合理性认定

聂 鑫
（南京理工大学 知识产权学院，江苏 南京 210094）

摘 要：云计算业已成为企业数字化转型的必然选择，作为信息存储处理技术的云计算出现与应用使得商业秘密保密措施合理性认定趋向复杂化。商业秘密信息管理权的部分移转使得云服务提供商进入认定考察视野，云服务提供商对“上云”信息内容接触权的保留及保密责任的明示排除，构成了保密措施合理性认定的障碍，传统的合理性认定之框架与方法有待重塑。基于保密措施的财产公示与防止过度保护的设定逻辑以及合理性之相对性与经济性内涵，结合促进云计算产业发展，遵循网络中立原则与考察权利人保密意思的因素考量，云计算环境下商业秘密保密措施合理性的认定应将信息“上云”行为做出信息移转与内容披露的类型化区分，在此基础上建构以信息“上云”行为的类型，云服务提供商是否负有保密义务，权利人采取保密措施情况为分析步骤的三步分析法。

关键词：云计算；保密措施；合理性；披露

中图分类号：D912.29 **文献标识码：**A **文章编号：**1009-0150(2022)05-0138-15

一、引 言

自2006年云计算概念的首次提出以来，云计算经历了从概念层面到商业层面的飞速发展。现今的云计算涵盖了“云端”上的硬件设施、开发平台以及软件应用等多类型化的服务形式。基于云计算技术开发的云服务产品，如Icloud、Onedrive、Gmail，已是人们进行日常邮件传递、信息存储、在线教育等活动的必备工具。凭借信息存储处理的低成本、便利性、自动化等优势，云计算已成为企业数字化转型的必然选择，越来越多的企业将其数据和信息迁移到“云端”（后简称为信息“上云”）存储处理。[①]特别是近年来，新冠肺炎疫情的出现，进一步激发了企业利用云服务进行信息存储处理的内生需求，云计算的市场规模也不断扩大。[②]由于企业“上云”的信息很多都是不对外公开的，属于商业秘密的范畴，云计算的推广与普及不可避免地给商业秘密保护提出了新挑战，其中最为突出的就是权利人采取保密措施的合理性认定问题。[③]我国《反不正

收稿日期：2022-06-21

基金项目：国家社会科学基金项目“少数民族非物质文化遗产知识产权保护制度创新研究”（20BMZ083）；教育部人文社会科学研究青年基金项目“大数据时代商业秘密民事法律制度应对研究”（17YJC820040）。

作者简介：聂 鑫（1983— ），女，湖南邵阳人，南京理工大学知识产权学院副教授、硕士生导师。

①Audra A. Dial, John M. Moye. Trade Secrets in the Cloud: Assessing and Mitigating the Risks, Journal of Internet Law, 17, 2014, p. 2.

②据统计，2020年，全球云计算市场规模已达到2083亿美元，近5年的年平均增长率保持在21.22%，预计到2023年全球市场规模将超过3500亿美元。我国云计算同样发展较快，2020年的整体市场规模达到了2091亿元。中国信息通信研究院：《云计算白皮书》，第1页，http://www.caict.ac.cn/kxyj/qwfb/bps/202107/P020210727458966329996.pdf。

③如在新丽传媒诉派华文化案中，双方当事人争议的焦点之一就是被告将原告商业秘密信息上传百度网盘进行存储处理的行为是否构成保密措施不当。北京市朝阳区人民法院〔2017〕京民初第68514号民事判决书。

当竞争法》第十条第三款的规定明确将权利人对商业信息采取相应“保密措施”设定为商业秘密构成要件，将其作为获得商业秘密保护的前提条件之一。2020年修订的《最高人民法院关于审理不正当竞争民事案件应用法律若干问题的解释》第十一条对“保密措施”又作出了进一步解释，要求权利人为防止信息泄露所采取的保密措施必须达到合理程度，并将限制涉密信息的知悉范围和设定保密责任作为认定合理性的重要考量因素。云计算环境下权利人将商业秘密信息“上云”，意味着将管理权的一部分让渡给了云服务提供商，权利人只能通过网络接口对商业秘密进行管理，商业秘密信息的安全管理主要依赖于云服务提供商。而云服务提供商对“云端”信息的以下管理方式，形成了保密措施合理性认定的障碍：一是内容接触权的保留。云计算环境下部分云服务提供商通常会保留对权利人（用户）存储全部或者部分信息的访问和利用权利。换言之，权利人将商业秘密信息“上云”，进行存储处理过程，并非简单的“人机交互”，存在向云服务提供商或其他第三方披露，无限扩大了涉密信息知悉范围的风险。[①]二是保密责任的明示排除。在交易对象或合作方必须知悉涉密信息的情况下，与知悉商业秘密内容的主体签订保密协议也是作为认定权利人采取合理保密措施的情形之一，但是云计算环境下云服务提供商通常会凭借与用户（特别是中小企业）交易谈判中的强势地位，通过格式合同，明确排除对用户存储信息保密责任的承担。[②]基于现有认定框架与标准，“上云”信息将难以满足保密措施的合理性要求，获得商业秘密保护的资格，如果放宽认定标准，则会消解“保密措施”作为商业秘密构成要件的防止过度保护、财产公示的作用。因此，云计算环境下商业秘密保密措施的合理性认定既是云计算这一新兴商业模式所面临的首要法律障碍，也是商业秘密法在新技术条件下如何发展的新问题，值得深入探讨。

云计算环境下商业秘密保密措施的合理性认定问题已在国外引发了学界和实务界的热烈讨论。国外有学者认为，企业如将商业秘密信息“上云”，将对保密措施的合理性认定构成否定性评价，相关涉密信息还是否能以商业秘密方式进行保护将受到严重质疑。[③]但是大部分学者认为，云计算环境下云服务提供商虽然可能知悉企业“上云”涉密信息的内容，并且其在云服务协议中明示排除相应保密责任，但仍不能简单据以认定企业没有采取保密措施，从而使相关涉密信息丧失商业秘密的保护基础，而是应该遵循个案考察原则。[④]对该问题的争论，还表现为司法实践中法官对于合理性认定标准的把握，如在Amedisys Holding v. Interim Healthcare of Atlanta案中，主审法官认为对于保密文件的限制访问以及通过受保护的电脑和邮件系统进行信息传输就足以表明保密措施的合理性。[⑤]而在G. W. Henssler & Associates v. Marietta Wealth Management案中，主审法官则认为仅对信息进行密码保护和访问限制难以被认定为合理，还需

①谷歌公司制定的适用云产品（如Gmail、Google Docs）服务协议中规定：“当您上传或者提交信息内容到我们的产品，意味着您授予了谷歌（以及与我们合作的公司）在全球范围内使用、存储、复制、修改、创作衍生作品（如翻译）、沟通、发布、公开播放、公开展示和分发此类内容的许可。您在本许可中授予的权利仅用于经营、推广和改进我们的服务以及开发新服务的有限目的。”Google Terms of Service, http://www.google.com/policies/terms, 2022年8月8日访问。

②亚马逊公司制定的云产品用户协议规定：“我们努力确保您的内容安全，但鉴于互联网的性质，我们不能保证我们能成功做到这一点。您对于我们产品的使用意味着您将单独承担对于您内容和应用程序的充分安全、保护和备份的全部责任。对于您任何内容或应用程序未经授权的访问或使用、损坏、删除、销毁或丢失，我们将不承担任何责任。”AWS Customer Agreement, AMAZONWEB SERVICE, http://web.archive.org/web/20090831034111tp://aws.amazon.com/agreement,2022年8月8日访问。

③Lennin Hernandez Gonzalez. Trade Secret Protection in the Cloud, February 8, 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2912905, 2022年8月8日访问。

④Sandra Wachter, Brent Mittelstadt. A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI, Columbia Business Law Review, 2019, 2019, p. 494.

⑤Amedisys Holding, LLC v. Interim Healthcare of Atlanta, Inc, 793 F. Supp. 2d 1302, 1311(N.D. Ga. 2011)

要与相关员工签订保密协议。[①]相较于国外，目前国内对此问题的研究较少，虽有学者的研究关注到了云计算环境下商业秘密保密措施的合理性认定问题，但更多偏向宏观视角，将此问题纳入云计算环境下商业秘密保护的系统性问题中进行探讨，缺少对合理性认定所涉相关理论问题，尤其是认定路径和方案建构问题的深入分析与探究。[②]

鉴于此，本文首先从探究云计算作为信息存储处理技术的缘起、类型以及价值出发，解析云计算环境下商业秘密保密措施合理性认定的实践场景以及问题表现；其次，讨论与分析商业秘密保密措施的设定逻辑与合理性内涵，为合理性认定的分析架构建立、标准设计、方法确定提供理论依据；最后，基于云计算环境下法律价值的考量，对信息“上云”行为进行类型化区分，并以此为基础，结合保密措施的合理性内涵，建构商业秘密保密措施合理性认定的分析框架及方法，以裨益于我国商业秘密立法完善以及司法实践。在此过程中，本文可能的创新之处主要有以下三方面：一是不同于既有研究的宏观视角偏向，本文以商业秘密保密措施合理性认定的微观视角切入“上云”信息商业秘密保护的关键性问题，力图在云计算环境下探寻破解商业秘密保护法律障碍的具体方案；二是基于商业秘密保密措施的设定逻辑，结合国外相关典型判例，从相对性与经济性两维度，探析保密措施合理性的理论本质与内涵；三是建构以信息“上云”行为类型化为基础的保密措施合理性认定框架及分析方法，为云计算环境下我国商业秘密保密措施的合理性认定提供方案参考。

二、作为信息储存处理技术的云计算

云计算是一种基于互联网，以服务形式向用户共享计算能力、存储空间和信息服务的架构安排。[③]作为信息存储与处理技术的云计算，并不是一个新概念。早在20世纪50年代计算机产业刚刚兴起时，由于处理和存储信息只能在大型计算机中进行，考虑到购买和维护大型计算机的高昂成本，当时就有计算机专家提出了“虚拟化”概念，认为大多数计算机中存在着的过剩计算能力可供其他人分享使用，只要计算机之间传输数据的技术难题能够得到解决。[④] 20世纪60年代末期，就出现了专门为大型机构和企业提供租用计算机主机或者数据存储服务的企业，如IBM公司、雷明顿兰德公司。[⑤]随着20世纪80年代计算机技术的发展，特别是互联网的出现，不仅使得个人计算机具备了信息处理与存储能力，也让计算机之间实现了网络互联，计算机终端朝着智能化、“去中心化”的方向发展，进一步为信息存储与数据处理能力的共享提供了技术铺垫。2006年，Google首席执行官埃里克·施密特在全球搜索引擎大会上开创式地将云计算作为概念提出，同年亚马逊首次将其弹性计算能力作为云服务推出，标志着云计算作为概念与商业模式的正式诞生。

现今网络技术的进一步发展使得云计算已超越了单纯的技术范畴，而演变为一种以第三

①G. W. Henssler & Associates, Ltd. v. Marietta Wealth Management, KKC, 2017 WL 6996372, at * 4 (N. D. Ga. 2017)

②笔者于2022年6月14日，以“云计算”与“商业秘密”为主题词在中国知网进行检索，共检索32篇期刊文献，其中较有代表性论文包括：周铭川：《云服务用户商业秘密的法律保护》，《暨南学报（哲学社会科学版）》2014年第1期；闫文军：《云计算环境下商业秘密保护问题探讨》，《电子知识产权》2013年第6期；董少平：《云计算知识产权问题研究》，《科技进步与对策》2014年第9期；罗先觉、尹锋林：《云计算对知识产权保护的若干影响》，《知识产权》2012年第4期。

③刘鹏：《云计算》（第三版），电子工业出版社2015版，第1-3页。

④John McCarthy. Reminiscences on the Theory of Time-Sharing, May 1, 1974, http://jmc.stanford.edu/computing-science/timesharing.html, 2022年8月8日访问。

⑤Ishaq Zakari. History of Computer and its Generations, October 10, 2019, https://www.researchgate.net/publication/336700280, 2022年8月8日访问。

方提供服务的形式向用户按需提供资源池的技术理念。具体而言，该理念的基本内容是存在一个提供托管服务的虚拟基础设施，用户可以通过网络，利用托管服务，无处不在、按需调用远程存储在主机服务器（“云”）上的资源与信息。随着云计算技术的发展，逐渐也扩展出多重的云服务模式。早期的云服务模式为“软件即服务”（software as a service）。在该模式下，云服务提供商通过互联网提供特定的应用程序，这些应用程序常用于电子邮件、备份或损坏修复、存储服务，如提供在线社交服务的Facebook、网络邮件服务Gmail，以及文件存储服务的ICloud。广义而言，任何可以通过Internet访问远程服务器上的应用程序都可以视为“软件即服务”模式。随后又出现了“平台即服务”（platform as a service）模式，这是一种由云服务提供商提供硬件和操作系统等应用工具，以便用户开发或部署自己应用程序的云服务模式，如谷歌的App Engine。除此之外，还出现了“基础设施即服务”（infrastructure as a service）。该模式下，用户可以访问可扩展的诸如硬件设备、网络组件等基础资源，如Amazon EC2和S3。值得注意的是，不同云计算的服务模式之间有着相互渗透融合的发展趋势，某一种产品可横跨两种以上模式，尤其在“基础设施即服务”与“平台即服务”之间。[①]

云计算的出现给用户的商业信息存储处理带来了重要价值，主要体现为：（1）低成本。资源与技术支持由云服务提供商提供，用户无需再投入大量资金用于计算机服务的软件、硬件采购与维持，也无需支出用于实施与维持计算机基础设施的人力成本。此外，云计算的应用还可以为用户节约用于存放服务器的空间等运营管理成本。（2）便利性。随着网络带宽和互联网基础设施的拓展，云计算可以提供给任何用户对信息的“即时存取”的特性，该特性能让用户的员工能够随地、随时工作，极大提升企业的生产效率。[②]（3）可靠性。云计算还提供给了用户一种用于存储和保存商业信息的可靠方式。用户可以在“云端”上以较低成本上传、存储和保持海量信息。另外，基于云存储的分散性特点，相对于存储在实体服务器中的数据，云数据不易丢失和删除，通常也有更长的保存时间。基于以上优势，企业将商业信息“上云”已成为不可逆的趋势。

云计算在带来低成本、便利性的同时，信息安全问题亦不可忽略。云计算环境下信息的存储处理安全性完全都由云服务提供商所管理控制，用户甚至不知道信息具体存放的确切位置，信息安全成为用户的最大顾虑。[③]基于信息安全问题，虽然有学者建议企业不要将商业秘密信息上云，[④]但是在企业数字化转型的背景下，企业将商业秘密信息上云具有强烈的内生需求，原因如下：一是很多商业秘密形成于企业日常经营活动，信息存储处理要满足员工日常存取需求，如客户名单信息，而云计算的便利性正好契合了这一需求；二是多数中小企业基于资金实力的欠缺，缺少架设私有云的能力，为减少设备成本开销，即便存在潜在的安全风险，还是会选择云服务进行商业秘密信息存储处理。故此，如果“上云”信息涉及商业秘密，基于上文所述的云服务提供商管理方式，这些信息还能否满足商业秘密保密措施的合理性认定要求，就成为了关键性问题。云计算的出现与应用所引发的保密措施合理性争议，已不仅是理论层面的探究，而是已经发生的事实。美国Wayman Fire Protection, INC., v. Premium Fire & Security, LLC就是

①[英]克里斯托弗·米勒德：《云计算法律》，陈媛媛译，法律出版社2019年版，第5-6页。

②Lisa Angelo. Exploring Legal Issues at High Altitudes: The Law in the Cloud, Currents International Trade Law Journal, 20, 2012, p. 41.

③根据美国华盛顿大学TechCast中心对云计算服务的调查显示，对安全问题的关切排在第一位，占比70%。Tim Gibson, On Cloud Computing. May 8, 2013, http://www.docin.com/p-649041030.html. 2022年8月8日访问。

④Alexis Salerno. Protection “Crown Jewel” Trade Secrets in the Cloud though Voluntary Industry-Government Collaborations and Federal legislation, 21 DePaul Business & Commercial Law Journal, 21, 2018, p. 442.

其中一例典型案件。[①]在该案中，被告Premium Fire是一家专门从事火灾报警与消防系统的企业。该企业相继聘用了原告Wayman的多位离职员工，专门从事市场业务拓展工作。在其中一位员工离职之前，保留了原告发放用于备份文件的U盘，并使用工作电脑登录Dropbox账户，下载了多份文件到其U盘之中。在被告处工作后，为了工作便利，该员工将下载文件复制到被告为其发放的工作电脑之中进行使用。另一位离职员工在原告工作期间，使用一个外部硬盘来备份原告工作电脑上的文件，把硬盘中的17000份文件内容复制到被告为其发放的电脑中，这其中就包括一份客户报告和一份销售可行性报告，以上两份报告均由原告使用的客户关系管理工具软件“Salesforce”生成。原告不仅使用该工具软件存储客户相关信息，如客户合同信息、销售信息和提案信息，每年还向该软件公司支付15000美金使用费和数千美金定制化数据库以满足专门需求。该软件的登录设置有密码保护，并且软件用户30—60天就需要更改一次密码。这些安全措施均为“Salesforce”服务的一部分，而非为用户所定制。原告的该前员工承认使用了以上文件用于与老客户的接触。在被告获得多伊尔斯敦医院的火警消防系统升级项目后，原告开始怀疑其拥有并使用了其专有的程序文件，是故，聘请了一位计算机取证专家，调查其前雇员是否从其工作计算机上复制了相关文件带到被告处。基于调查结果，原告指控被告侵犯了其商业秘密。而被告的抗辩理由之一就是原告的商业秘密信息没有对涉密信息采取合理的保密措施，相关信息不能构成商业秘密。可见，法院在判定被告是否承担商业秘密侵权责任前，需要认定原告有无对涉密信息采取合理的保密措施。

三、保密措施的设定逻辑与合理性内涵

（一）保密措施的设定逻辑

保密措施是商业秘密构成的重要要件之一，要求商业秘密权人为防止涉密信息泄露，不仅对涉密信息要有主观保密的意图，还需对该信息采取客观上的积极保护措施。保密措施对于商业秘密的产权属性形成具有重要的意义。“财产法的形式主义要求，一个客体要成为财产法律规范的客体，必须具备客观上能够进行专有性、排他性占有的外部特征。只有个性化的个体与个别性的物相互占有才有对抗他人的公信力”。动产物权的排他性占有外部特征为所有权人对物的交付与有形控有，不动产物权则为登记。商业秘密权与物权同属绝对权，具有同样的公信力与排他性需求。[②]商业秘密作为知识产品的类型之一，非物质性是其本质特征。就性质而言，客观上不是“个别性”的存在，没有排他性“占有”的外部特征，其自身没有公示效果，所以必须借助一种外在的强制力量赋予知识排他性占有的外部特征，使其具有公信力，从而使其财产化。这种强制的外部力量不可能来源于知识生产者自己，也不可能来源于私权地位的其他个人或者团体，而只能来源于使知识排他性占有的外部特征以及相应的公信力具有普遍意义和强制效果的法律。[③]保密措施就是商业秘密被法律赋予知识排他性占有的外部特征。法律要求商业秘密权人采取由内表现于外的客观保密措施，能够在一定程度上建构其商业秘密的物理“栅栏”，起到类似物权的排他性占有和相应公信力的效果。

保密措施还是商业秘密产权形成过程中防止过度保护的衡平工具。社会在确定某一资源是否适宜设置产权保护的重要依据是收益与成本的比较，只有当确定产权的收益超过成本时，

①Wayman Fire Protection, Inc. v. Premium Fire & Security, LLC, 2014 WL 897223 (Del. Ch. 2014), 2014 WL 2967749 (Del. Ch. 2014).

②吴汉东：《知识产权基本问题研究（第二版）（分论）》，中国人民大学出版社2009年版，第596-597页。

③李扬：《知识产权法基本原理（Ⅰ）—基础理论》，中国社会科学出版社2013年版，第16页。

在某一资源上设定产权保护才具有经济学上的意义。正如罗伯特•考特与托马斯•尤伦教授所言：“授予思想以产权的法律。在此，如同易逝的资产一样，法律必须在先占原则下，在过度投资的刺激与在别的制度下管理和履行所有权所需的较高成本之间加以权衡。”[①]商业秘密保护就涉及信息的私人占有与公众的信息利用之间的收益成本平衡问题。信息的公开及自由传播既是民主政治的象征，也是促进科技与经济发展的前提。虽然授予商业秘密产权利于保护权利人的合法权益、维持商业道德、促进市场竞争秩序的公平，但是商业秘密以秘密性为特点，决定了其与专利保护存在较大区别，专利权的授予是专利技术持有人以向社会公开作为对价换取，并且专利权之上还附加时间限制，即使专利权被设定有较强的排他性，也不会影响个人私权与社会公益之间的利益平衡。商业秘密信息不向社会公开获得产权保护，只要持有人不向社会公开信息内容，社会公众亦不能从商业秘密的保护获得资源，对于商业秘密的过度保护可能损及社会公共利益，造成社会资源的净损失。[②]是故，法律严格限制授予商业秘密产权保护的客体范围，而保密措施就是限制工具之一。采取保密措施实际上是商业秘密权人向他人表明对商业秘密信息占有主观意图的方式。根据保密措施的要件要求，如果商业秘密信息拥有人不能证明自己对信息采取的保密措施达到合理程度，则其所主张的商业信息内容就不能得到法律的保护。因为如果信息拥有人自己对相关信息都没有主观“占有”的意思表示，证明该信息对其无价值，法律就没有设置产权保护的必要。[③]因此，保密措施的限制性作用主要体现在将无价值的信息排除到产权保护范围之外。

基于在商业秘密产权形成中的作用，很多国家司法实践中，将保密措施作为认定权利人能否获得商业秘密保护的头等要件。[④]

（二）保密措施之合理性内涵

不同类型产权的排他性强弱决定了相应获权的难易。基于私人占有与公众的信息利用的利益平衡考量，授予商业秘密产权的排他性要小于专利权，商业秘密权人仅能根据先用原则享有商业信息的部分利益，不能对抗独立研发和反向工程。[⑤]由此，法律对于保密措施的要求，并非要“万无一失”，仅达到合理性程度即可。那何为保密措施的合理性？目前对于合理性的内涵界定尚无定论。笔者认为，保密措施的合理性主要体现为以下两方面。

一是合理之相对性。对于保密措施的合理性内涵界定，依存于特定的场景和环境。不同个案中的当事人、时间、地点、商业秘密性质等情况，均是合理性内涵界定的因素。一般情况下被视为契合合理性内涵要求的保密措施，在特殊情势下即使存在缺失或者转换也不必然导致保密措施被认定为不符合要求。如在H. Q. Milton v. Webster案中，针对被告以原告没有与员工签订保密协议，没有对计算机上存储的涉密信息加密等理由，主张原告没有采取合理保密措施的抗辩，法院尽管认可签订保密协议以及对信息进行加密处理是通常判断《保护商业秘密法》所规定保密措施合理与否的标准，但具体到本案中，考虑到原告已向员工示明了需要进行保密的信息内容，对存储涉密信息的计算机设置了密码保护，并且仅在员工范围内披露了涉密信息等

①[美]罗伯特•考特、托马斯•尤伦：《法和经济学》，张军译，上海三联书店1991年版，第185页。

②吴汉东：《知识产权基本问题研究（第二版）（分论）》，中国人民大学出版社2009年版，第601-602页。

③谢晓尧：《在经验与制度之间：不正当竞争司法案例类型化研究》，法律出版社2010年版，第398页。

④世界知识产权组织国际局：《世界反不公平竞争法的新发展》，郑友德等译，载漆多俊：《经济法论丛》（第1卷），中国方正出版社1998年版，第313页。

⑤Gordon L. Doerfer. The Limits of Trade Secret Law Imposed by Federal Patent and Antitrust Supremacy, Harvard Law Review, 80, 1967, p. 1462.

证据，最终得出原告采取保密措施达到合理性的结论。[①]正是合理性内涵具有相对性的意蕴，决定了保密措施被认为是商业秘密构成要件中最具弹性的要件，需要结合个案特殊情况界定。[②]

二是合理之经济性。保密措施的合理性与商业秘密信息的经济价值相关，是一种经济意义上的合理。商业秘密权人对于信息安全所采取防御措施的成本投入及程度，仅需大致与商业秘密信息的经济价值相当即可。竞争对手通常只会投入与商业秘密信息价值相匹配的资金、人力成本规避防御措施，获取相应的商业秘密信息，商业秘密权人也仅会投入与价值相对应的资金成本保护信息，因此商业信息的经济价值通常取决于商业秘密权人或者意欲获取商业信息竞争对手的评价。法律将经济价值设定为保密措施合理性内涵的原因是防止权利人在商业秘密信息保护方面的过度投资，从而造成创新削弱和效率低下，抑制“创新精神”。正如波斯纳法官所言，保密措施的合理性设定是一种平衡，即保持信息安全方面的额外利益是否会超过预期成本的平衡。法律不需要商业秘密权人采取过分的、不切实际的、削弱活动能力的“超合理”保密措施来维持信息的秘密。[③]如Christopher案中，法院对于合理性的认定就达到了这种平衡。原告杜邦公司并没有因为未在其建筑工地上方加盖顶棚这一事实，而被法院认定其采取的保密措施不合理，从而使得该工地上所进行任何事情都成为共同信息。该案中法院的认定不仅能阻却被告Christopher公司投入大量资金去租用飞机和飞行员探悉杜邦公司拥有商业秘密信息的内容，还能消除杜邦公司建造顶棚上花费资源的激励，从而打消竞争对手寻租的念头。[④]

四、认定前提：信息“上云”行为的类型化区分

对保密措施的合理性分析，取决于特定的场景、环境与条件。云计算环境下，用户将信息“上云”进行存储或处理，如上文所述，虽然信息的所有权仍在权利人手中，但是信息的管理权已由权利人部分让渡给了云服务提供商。对于信息“上云”行为的性质界定直接关系到云计算环境下保密措施合理性认定的考察方向及内容，是合理性认定的前提。而界定的关键就在于判断信息“上云”行为是否构成商业秘密法意义上的披露。所谓披露是指行为人以口头、书面或其他方式将商业秘密信息内容向特定人或不特定人进行传播、公布行为。[⑤]如果将用户信息“上云”行为判定为商业秘密法意义上的披露，即权利人向相关人主动而为的公开，保密措施合理性认定就会进而考察云服务提供商作为被公开对象的保密义务设定及其采取保密措施情况，而如将该行为仅视为信息管理方式的改变，不为披露，考察的重点将还在于商业秘密权人自身采取保密措施的情况。

（一）类型化基础：行为界定的价值考量

在云计算环境下对信息“上云”行为进行类型化区分界定，取决于相应法律的价值评价，理由如下：

一是保障云计算产业发展层面。作为规范社会成员行为及其相互交换规则的法律并不是存在于真空之中，基于科学技术或商业模式创新对于社会成员行为方式的影响与改变，法律制度要进行适应性确认、调整，以更好地实现制度规范功能。正如马克思在论述经济与法律的关系时说道：“每当工业和商业的发展创造出新的交往方式，法便不得不承认他们是获得财产的

①H.Q. Milton, Inc. v. Webster, 2017 WL 5625929 (N.D. Cal. 2017).

②Elizabeth A. Rowe. Saving Trade Secret Disclosures on the Internet Through Sequential Preservation, Wake Forest Law Review, 42, 2007, p. 1.

③Victoria A. Cundiff. Reasonable Measures to Protect Trade Secrets in a Digital Environment, Idea, 49, 2009, p. 359.

④[美]威廉• M.兰德斯、理查德•A. 波斯纳：《知识产权法的经济结构》，金海军译，北京大学出版社2005年版，第468页。

⑤根据我国《反不正当竞争法》第九条的规定，“披露”被视为第三人侵犯商业秘密的行为方式之一。

新方式”。知识产权法尤为如此，知识产权法从兴起到现在，历经从工业革命到信息革命的不同时期，“基于科技革命而生，由于科技革命而变”，制度发展史本身就是一个法律制度创新与科技创新相互作用、相互促进的过程。[①]云计算环境下，如果对商业秘密权人的信息“上云”行为不加区分地视为对云服务提供商或其他人的信息内容披露，对于保密措施合理性的认定，则要求考察云服务提供商是否附加有相应的保密义务。[②]如上文所述，基于云服务提供商排除保密责任的一般性做法，以及云服务提供商相对强势的谈判地位，特别是对中小企业而言，或者会极大增加因保密谈判而产生的交易成本，或者直接产生否定合理性的法律效果，最终对企业利用云产品和服务进行信息存储处理起到“寒蝉效应”，而这将对云计算产业的发展非常不利。[③]

二是遵循网络中立原则层面。网络中立原则最早由美国哥伦比亚大学的吴修铭（Tim Wu）教授于2003年提出，作为技术中立原则在互联网领域的适用，是指网络服务提供商应同等对待来自各方的内容，不对任何传输数据内容进行区别对待或干涉。目前该原则在全球互联网领域有着广泛的应用。[④]依据网络中立原则的理念，云计算环境下，云服务提供商向用户提供的仅是存储或处理服务，而并不在乎用户上传的内容本身。即便部分云服务提供商会保留对用户上传信息的内容接触权，但并不意味着云服务提供商会实然接触信息内容。云服务的中立性也符合用户的预期。据有学者调查显示，绝大部分的云服务用户对存储在第三方计算机服务器中的信息存在隐私的预期，认为存储“云端”信息不会被云服务提供商或者他人直接获取和知悉。[⑤]是故，相较于传统信息存储或处理方式，虽然云储存会存在更大的信息泄露风险，但是如果将权利人信息“上云”行为不加区分地认定为是权利人向云服务提供商进行信息内容的披露，则明显与网络中立原则的内涵要求不符。

三是考察权利人保密意思层面。商业秘密的秘密性要件主要考量信息的客观秘密性，对权利人而言，仅有信息的客观秘密性不足以获得法律保护，只有这种秘密性里蕴含了权利人的保密意识并外化为保密措施时才能得到法律认可。[⑥]而保密意思作为权利人的主观心态往往隐藏于内，需要通过相应外部可以感知的客观行为予以佐证。例如在浙大恩特公司诉吴某某等侵犯商业秘密一案中，法院认为商业秘密权人主观上具有将技术信息和经营信息作为商业秘密保护的意愿，客观上也采取了相应的保密措施，通过保密措施将其信息控制起来，使其不处于一种为公众所知悉的独占状态。[⑦]在云计算环境下，以商业秘密权人主观可预见的丧失秘密性风险为标准，对信息“上云”行为进行类型化区分，赋予不同的行为以不同的法律效果，继而对权利人提出不同程度的保密要求，以此建构主客观相统一的保密措施合理性分析架构。

（二）类型化区分：信息移转与内容披露

云计算环境下，对于信息“上云”行为的界定，需要回归云计算的技术本质，并结合相关价值考量进行类型化分析。云计算之“云”并非指的云服务提供商本身，而是云服务提供商基于互

①吴汉东：《知识产权多维度解读》，北京大学出版社2008年版，第84页。

②《最高人民法院关于审理侵犯商业秘密民事案件适用法律若干问题的规定》（法释〔2020〕7号）第六条明确将“签订保密协议或者在合同中约定保密义务”作为判断权利人披露信息时，认定合理性的重要因素。

③据统计，2021年，我国企业上云率仍然较低，上云率最高的北京市和广东省企业仅为9.4%，很多地区不足5%，企业上云率低的其中主要原因是担心数据、隐私等安全问题，该因素在暂无引入云计算计划的考量因素中占比41.3%。忆欧智库：“2021中国企业上云指数洞察报告”，第23页，https://pdf.dfcfw.com/pdf/H3_AP202203101551759055_1.pdf? 1646931193000.pdf.

④梁志文：《云计算、技术中立与版权责任》，《法学》2011年第3期，第87页。

⑤Matthew Tokson. Automation and the Fourth Amendment, Iowa Law Review, 96, 2011, p. 581.

⑥孔祥俊：《商业秘密司法保护实务》，中国法制出版社2012年版，第142-143页。

⑦浙江省杭州市中级人民法院〔2006〕杭民三初字第50号民事判决书。

联网技术建构，按需提供的远程软硬件资源平台。云服务提供商只是“云”平台的搭建、运营与管理主体。如上文所述，云服务提供商虽然保留了对“上云”信息的内容接触权利，但是基于接触的条件限定性以及海量信息的提取可能性，并不意味着其必然会对“上云”的信息内容进行接触。此外，区别于传统网络环境下商业秘密存放的整体式特点，云计算环境下的信息存放具有分散性特点。在“云”的大规模分布式存储机制中，权利人上传的完整数据通常被打散成不同的“碎片”存储在不同的服务器之中，他人要想获悉数据内容，必须基于大量存储服务器的访问授权，而这通常是非常困难的。[①]是故，权利人对于信息的“上云”行为并非意味着将信息内容直接向云服务提供商或他人进行了分享或者公开，亦可能只是通过人机交互，移转信息存储处理位置而已。

根据信息“上云”的用户目的与预期，以及云服务提供商对于“上云”信息的访问能力、内容知悉情况差异，宜将该行为区分为以下两种类型：一是信息移转式“上云”。权利人实施此种类型“上云”行为的目的是进行信息的备份存储和处理，没有向云服务提供商或者他人进行信息内容披露的主观预期，并且“上云”信息的交互与管理过程高度“自动化”，是一种人机交互，过程之中没有云服务提供商的干预或介入，信息内容也没有实际被云服务提供商所知悉。云计算环境下此种类型的信息储存处理与传统网络时代性质上并无二异，只是存在传统信息存储和处理的位置差异，由物理层面的计算机或服务器移转到了虚拟层面的“云端”。权利人实施信息移转式“上云”行为，既没有信息内容披露的主观预期心态，也没有云服务提供商或他人对信息内容知悉的既成客观事实，因此，并不构成商业秘密法意义上的披露。二是内容披露式“上云”。权利人实施内容披露式“上云”行为的目的在于利用云计算的便利性，与不特定的第三方进行信息协作或交流。权利人没有对云服务提供商进行信息保密的主观预期，并且信息“上云”的交互与管理过程存在云服务提供商的人为介入或干预，云服务提供商对于信息内容处于实际知悉的状态。内容披露式“上云”由于权利人向云服务提供商进行了内容的分享与披露，故构成商业秘密法意义上的披露。

五、适配类型化区分：合理性认定的分析框架建构

信息“上云”行为的不同类型界定具有重要的商业秘密法意义，直接决定了保密措施合理性认定的不同分析方向及考量因素。是故，云计算环境下的商业秘密保密措施合理性认定，应适配信息“上云”行为的类型化区分，建立相应的分析框架以及方法。

（一）信息移转或内容披露：信息“上云”行为的类型判定

随着云计算产业的纵深发展，云产品也日趋多样，用户对于云产品的利用方式和环境也在不断变化，基于信息“上云”行为类型界定对合理性认定的导向性作用，对该行为类型的判断不宜简单进行是非判定，而应适用“因素分析法”，在个案中结合具体案件事实，综合考量用户与云服务环境等多方面主客观因素，以防止合理性标准设定得过宽或过严。笔者认为，对于信息“上云”行为的类型判断，应考量以下三方面的因素。

一是权利人的主观合理期待。隐私合理期待是美国一项重要的隐私判断标准理论，源自《美国宪法第四修正案》中对公民财产权保护范围扩张的相关规定，在美国司法实践中有着广泛的运用。根据该理论，法律在判断何种隐私利益应受保护时，首先要考虑不同场景中权利人的合理期待，即自身是否希望该利益受到保护，如果权利人将自身的秘密公开，就不得再对该

①虚拟化与云计算小组编：《虚拟化与云计算》，电子工业出版社2009年版，第21页。

利益主张隐私的合理期待。[①]正如审理Katz v. United States案的Harlan大法官就曾指出“在大庭广众下所为的行为和陈述不应被保护，因为这些行为和陈述仅仅留存于自己这一期待并未被展现出来”。[②]目前隐私合理期待理论已为越来越多的大陆法系国家通过判例所接受，并且适用范围越来越宽泛，已扩展成为确定商业和其他领域隐私保护的标准，在划定公共领域与私人领域之间的界限方面具有重要意义。[③]商业秘密信息作为商业领域的一种隐私利益，该理论同样具有适用性。对权利人主观合理期待考量应作为信息“上云”行为类型判定的首要因素。如果权利人对“上云”信息有着对云服务提供商或者他人隐私保护的主观合理期待就应为信息移转，否则，则为内容披露。对权利人主观合理期待的考察，具体可包括两方面内容：第一，权利人的主观使用目的。如果权利人使用云服务产品的主观目的是单纯为了信息存储备份或者独立利用平台资源进行信息处理，而非在“云端”进行信息交流或者与云服务提供商进行交互式协作处理，就表明其主观上保留有一定的隐私合理期待。如在Gmail案中，谷歌公司认为用户使用邮箱服务就应该知道邮箱在扫描垃圾邮件时邮箱服务提供商就会知悉邮件内容，因此，不应对被扫描的邮件数据保有合理的隐私期待，但是法院否定了该主张，认为该主张超过了用户的一般主观预期和常识。[④]第二，用户的客观行为表现。对于权利人主观合理期待的考量亦可通过个案中权利人具体使用云产品的行为证据予以佐证。如权利人在选择云服务产品存储商业秘密信息之前是否开展过云服务产品安全等级调查和评估，权利人在云产品的使用过程中是否充分利用过云产品中内置的信息安全保障措施等行为，都可以作为考察权利人有无信息隐私合理预期的行为证据。

二是云服务产品的环境设定。云服务产品的环境设定是分析云服务提供商对“上云”信息接触、使用、利用方式与范围的客观依据，亦是权利人作出信息“上云”决策的重要考量，故此，该因素是评价与界定信息“上云”行为类型的重要维度。对该因素的分析，具体可包括以下两方面：(1)云服务提供商对服务的相应声明。如上文所述，虽然用户协议中的声明通常会排除对于权利人“上云”信息的安全保障责任，正是这种明确对保密责任排除的意思表示，权利人的保密义务很难被认定，但云服务提供商在服务声明中的意思表示并非没有任何意义。由于该声明作为权利人与云服务提供商之间订立的服务协议内容，应当视为权利人对相关认可和确认，其可以作为判断“上云”信息是否可能或者在何种程度或范围被云服务提供商收集、访问或者使用，继而作为判断信息披露或内容披露的依据。(2)云服务提供商地位与作用。考察云服务提供商在信息“上云”中的作用。一些云服务产品，特别是云存储服务大多都是一种高度自动化的，没有云服务提供商的人为干预，就应为信息移转，而另一些产品则依赖于人为的干预，需要获取消费者的个人信息，如华为云关于漏洞扫描服务作出的声明内容表示，如果用户利用该漏洞扫描服务，就相当于同意授权其收集和使用用户“上云”的个人信息或个人敏感信息的权利，基于该授权，华为云的服务提供商会出于上述目的分析使用这些信息。[⑤]而如果通过干预，相关信息内容被云服务提供商知悉，那就应为内容披露。

三是信息被实际知悉情况。如上文所述，云计算环境下，虽然云服务提供商可能会保留对

①张民安：《美国当代隐私权研究》，中山大学出版社2013年版，第449页。

②王利明：《王利明学术文集•人格篇》，北京大学出版社2020年版，第605-610页。

③有学者认为，鉴于我国《民法典》的第一千零三十二条现已明确规定了隐私权的概念，为隐私权的界定提供了相对明确的标准，因此，虽然我国无必要在法律中引入隐私合理期待理论，但是法官仍可在借鉴该理论的基础上具体判断哪些利益应当受到隐私权保护。王利明：《王利明学术文集•人格篇》，北京大学出版社2020年版，第630页。

④In re Google Inc. Gmail Litig., 936 F. Supp. 2d 1381, 2013 U.S. Dist. LEXIS 49251 (J.P.M.L., 2013).

⑤《华为云漏洞扫描服务声明》，https://www.huaweicloud.com/declaration/vss_sas.html，2022年8月8日访问。

“上云”信息的内容接触权，但是权利保留并不等于实际接触，其对于上云信息的知悉可以区分为以下几种情况：(1)基于用户协议条款内容的限制，不能对“上云”信息进行接触或知悉；(2)未对“上云”信息内容的接触权进行保留，并且也未对信息有任何接触或知悉；(3)基于权利保留，在特定条件下，具有对“上云”信息内容接触、使用的权利，但由于条件未具备或者海量信息提取困难等原因，对信息没有实际的知悉或接触；(4)有权对“上云”信息进行接触或知悉情况下，已经对相关信息实际接触或使用。区别于信息移转式“上云”仅为信息存储处理位置的移转，内容披露式“上云”是用户构成对云服务提供商就“上云”信息实然的内容披露，故此，只有权利人的信息“上云”构成了第四种类型的知悉，才应被认定为内容披露，否则，仅为信息移转。

通过综合以上因素的考量，如果将权利人信息“上云”行为判定为信息移转，意味着权利人并未就涉密信息与云服务提供商进行过分享和披露，合理性认定则应直接进入第三个步骤，对于权利人采取保密措施情况的分析。而如将信息“上云”行为判定为内容披露，合理性认定则应继而进入第二个步骤的分析，即对于云服务提供商是否负有保密义务的考察。

(二)云服务提供商是否负有保密义务

商业秘密权人就涉密信息向他人进行内容披露并不直接意味着保密措施的缺失，一项商业秘密一般是在一定范围内为特定的人员所知悉并使用，[①]如雇员、签订有保密协议的合作伙伴等，只有权利人将信息内容披露给没有任何保密义务和责任的第三人才可能被认定为未采取合理保密措施，进而导致商业秘密权利的丧失。美国联邦最高法院曾在审理Ruckelshaus v. Monsant案的过程中指出：“如果在没有任何保密责任情况下权利人自愿公开将涉密信息披露给非雇员的第三人，权利人对该信息的财产权利将会灭失。”[②]我国《最高人民法院关于审理不正当竞争民事案件应用法律若干问题的解释》第十一条也明确将限制涉密信息的知悉范围和设定保密责任作为判断权利人是否采取保密措施的考量情形。是故，云计算环境下，如果商业秘密权人将“上云”信息以内容披露形式，让云服务提供商知悉，合理性认定需要进一步考察云服务提供商是否负有保密义务。

商业秘密的保密义务主要可以区分为明示和默示两种类型。明示保密义务通常以当事人之间达成保密协议或条款的形式确定，协议或条款内容一般涉及保密信息范围、保密主体、保密期限等。云计算环境下，有少数云产品服务提供商会通过服务协议，明确承诺对于用户“上云”信息的保密义务和责任，构成对用户的明示保密义务。如在《腾讯云服务协议》的第八条中，云服务提供商不仅对保密信息的内容作出了界定，还明确了云服务提供商作为信息接受方的保密义务，规定未经信息披露方的书面同意，接受方不得以任何方式将保密信息披露给第三方或者用于本协议之外的目的，否则，违反保密义务给披露方造成损失，接收方应就披露方的直接经济损失作出赔偿。[③]大部分的云服务提供商仅会作出采取保密措施的承诺，但是如上文所述，同时他们会排除对于用户“上云”信息保密责任，基于这一明确的意思表示，云服务提供商将难以构成对于权利人的明示保密义务。

在缺少明示保密义务的情况下，法院通常还会考察一方当事人是否负有对另一方的默示保密义务。所谓默示保密义务是虽无明示的言辞，但从当事人之间关系、交易目的和法律规定

①杨力：《商业秘密侵权认定研究》，法律出版社2016版，第84页。

②Ruckelshaus v. Monsanto Co., 467 U. S. 986. 1002 (1984).

③《腾讯云服务协议》，https://cloud.tencent.com/document/product/301/1967#.E7.AC.AC.E5.85.AB.E6.9D.A1-.E4.BF.9D.E5.AF.86.E4.BF.A1.E6.81.AF，2022年8月8日访问。

而推断出的保密义务。[①]值得注意的是，有学者认为在我国没有必要承认默示保密义务，[②]但是无论从理论依据层面，当事人履行诚实原则、忠实义务的要求，还是从法律依据层面，《民法典》关于合同履行过程中以及终止后当事人的保密义务规定，默示保密义务在我国都有存在的依据和基础。[③]云计算环境下，权利人与云服务提供商之间的关系通常难以构成诸如雇佣关系、代理关系、合伙关系等产生默示保密义务的特殊保密关系。就交易目的或习惯而言，重点考察商业秘密权人是否为特定交易目的向云服务提供商披露涉密信息内容，如为安全目的的漏洞扫描等，云服务提供商往往受该目的的约束。虽然根据国外相关判例，即便信息接受者明示的保密义务排除，基于个案中的事实与环境，云服务提供商仍可能构成对于用户默示保密义务的特例。如在Burten v. Milton Bradle案中，信息接收受者在披露协议（disclosure agreement）中明示排除了保密义务，法院认为如事实证明披露是交易一方为了促进一种特定交易关系向潜在交易方披露，使其能够评估机密的价值，则潜在交易方有义务对接收到的信息保密。[④]但是一般而言，如果云服务提供商在用户协议中有对于保密义务排除的明确意思表示，就难以符合合同法意义上默示承诺的构成要求，不能构成默示保密协议。[⑤]

基于司法实践中云服务提供商保密责任和义务构成认定的困难，是否可以根据网络信息安全相关立法规定，作出扩张性解释，对云服务提供商施以法定的保密义务？如我国《网络安全法》第四十条、四十二条明确规定，网络运营者应对收集的用户信息严格保密，不得泄露、损毁、丢失用户信息，并应采取相应的技术安全措施，保证用户信息的安全。笔者认为，这一做法似有不妥。原因如下：第一，如上文所述，保密措施应是商业秘密权人主观见之于客观建构的财产“物理栅栏”，对于商业秘密的产权属性构成具有重要作用。如果对云服务提供商附加法定保密义务，意味着无需权利人任何的主观保密意图，施以任何的客观行为就可达成另一方当事人的保密义务，这明显与保密措施的设定逻辑不符。第二，用户与云服务提供商之间是合同关系，由合同法所规范，遵循合同自由原则。根据该原则，民事主体对自己权利设定或对他人义务承担，应按照自己的自由意思决定。[⑥]如果对云服务提供商负担保密义务作出“一刀切”的认定，有违合同法的该项基本原则。第三，云服务提供商投入不同的资源、施以不同的注意程度对“上云”信息的隐私安全进行保护，本身就是区分不同等级与类型云服务产品的标准所在，如果对云服务提供商的保密义务作出统一性的法定要求，也不利于云计算产业的多样性、差异化发展。

（三）权利人采取保密措施情况

云计算环境下，由于权利人对信息的管理权存在部分让渡，合理性认定可能涉及云服务提供商是否负有保密义务的分析，但无论是信息移转式“上云”，还是云服务提供商负有保密义务下的内容披露式“上云”，最终都还需要回归到第三步，权利人自身保密措施情况的考察。只有经过该步骤的校验，才能最终得出权利人所采取保密措施是否具有合理性的结论。鉴于云计算环境下信息存储处理方式、特点以及不可预知的安全风险，法院在该步骤的考察中对于调查分析方向或重点的选取，更应侧重权利人适配商业秘密信息价值，为防止信息泄露所采取的保护

①薛波：《元照英美法词典》，北京大学出版社2003年版，第666页。

②孔祥俊：《商业秘密保护法原理》，中国法制出版社1999年版，第269页。

③汤茂仁：《保密义务与商业秘密侵权认定》，“知产力”公众号，2015年5月8日，https://www.zhichanli.com/p/1026584916，2022年8月8日访问。

④Burten v. Milton Bradle Coast763 F. 2d 461 (1st Cir. 1985).

⑤默示承诺具有严格的条件限定，必须要有法律规定或当事人约定，且受约人一般还未作出任何拒绝承诺的表示。史尚宽：《债法总论》，中国政法大学出版社2000年版，第27页。

⑥梁慧星：《民法总论》，法律出版社2001年版，第49页。

商业秘密信息的技术措施和流程，以及系统性的风险评估和防控措施，而不是传统基于物理设施的保密措施。具体而言，应包括以下情形：[①]

一是商业秘密信息的界定与区别管理。只有被管理的对象被确定时，才可能被施以具体的管理措施，故此，合理性认定最基本的条件是权利人使用某种载体对商业秘密内容予以明确界定并施以区别管理。[②]云计算环境下，信息以电子化载体形式呈现，权利人不仅应有将涉密信息当作商业秘密的主观意识，将商业秘密信息与其他非密信息进行明确的区别界定，在企业制定的内部信息管理政策中进行差别化对待，还应采取实际的保密措施落实该差别化政策。如在涉密信息内容中进行涉密等级的标注，对涉密信息进行归类存放、限制接触、加密隔离存储，否则，就会缺失合理性认定的基础。

二是企业以及产业特性。权利人所采取保密措施之合理是一种相对合理性而非绝对合理性，权利人的企业规模、服务或产品类型、企业的商业运作模式以及权利人所处的产业特性所建构的特殊环境是个案中法院判断相对合理性的重要依据和标准。权利人所采取的保密措施需要与其企业与产业特性相适配，如大型企业，相较于中小企业，拥有更加雄厚的经济实力，为防止商业秘密信息泄露，对于云服务产品的类型选择、相应技术措施的实施标准，明显不能等量齐观，通常有更高的要求。[③]技术密集型产业，相较于劳动密集型产业，由于技术对于竞争力提升有着更为显著的作用和意义，产业所属企业的发展更加依赖于技术信息的生产与存储，是故，对该产业领域的企业采取相应的保密措施标准亦要求更高。

三是商业秘密信息特点及适配措施。商业秘密信息类型多样，且特点不一，因此，并没有所谓通行有效的完美保密措施，只有适配商业秘密特点设置的保密措施，才能发挥有效的保密效果。如存储于“云端”的技术操作规程与客户名单，在信息利用人员范围、利用频次等方面就有较大差异，就要求权利人对于访问权限设置以及相应配套措施进行区别对待。云计算环境下，保密措施的类型主要包括以下几方面：(1)员工访问“云端”权限控制。基于网络的虚拟性，确认登录用户身份合法性是首要问题，权利人应对登录“云端”的密钥采取必要的保密措施，如有的企业给每个登录员工提供一个特定“云端”登录账号，每个账号分配以不同的信息访问权限，并与员工签订信息安全和披露协议，要求其对账户与密码等信息保密。(2)登录客户端的范围控制。由于用户的任何操作都会在客户端上留存痕迹，并可通过一定途径获得，因此，还应对“云端”的客户端进行必要的范围和使用方式限制，如有的企业严格限定登录“云端”的客户端场所，并严格禁止员工携带照相功能的手机与录制设备进入该场所。(3)商业秘密信息的伪饰。为防止保密措施被破解，还有企业将保密措施聚焦于商业秘密信息本身，对商业秘密信息进行伪饰，如在真实的商业秘密信息中设置陷阱，添加虚假的信息内容，或者设置假的文件掺杂其中。[④]需要注意的是，合理性所具有的相对性内涵决定保密措施的设置无需完美无缺。保密的目标不是绝对安全，因为信息的绝对安全将使信息有益的作用难以发挥，也是不切实际的。

四是所选措施已知风险防控。基于新技术环境下信息保护风险的不确定性，很多国家法院对于保密措施的合理性认定，已由传统偏重基于设施的保密措施的静态考察，转向到因应技术

①本文所列举的四方面情形内容虽然存在某种程度的内容重叠，但是仍应独立进行分析，以达到更为综合、全面、连续的合理性分析目的。

②孔祥俊：《商业秘密司法保护实务》，中国法制出版社2012年版，第145页。

③In re Innovative Constr. Sys., Inc., 793 F.2d 875, 884 (7th Cir. 1986).

④Elizabeth A. Rowe. Rats, Traps, and Trade Secrets, Boston College Law Review, 57, 2016, p. 412.

风险的技术措施和防控过程的动态考察。[①]云计算环境下，单一的技术措施在很多情况下并不充分，不符合合理性要求，如在新丽传媒诉派华文化案中，法院经审理认为，虽然派华公司利用百度网盘存储诉争《悟空传》电影的素材过程中设置了密码保护，但鉴于百度网盘的保密性较低，该保密措施的严密程度与涉案素材的价值相比，明显难以匹配，具有重大过失的主观过错。[②]是故，法院在认定合理性过程中，不仅应基于成本效益分析，考量权利人所采取的保密措施本身是否合理，还应要求其提供信息安全风险评估以及相应风险防控的证据，以确定其使用的保密策略或者措施是否可行。

六、结　语

保密措施合理性认定具有动态化、相对性特点，取决于个案中的特定环境、场景与条件。在云计算环境下，面对合理性认定出现的适应性问题，商业秘密立法需要因应这一新场景的转换，及时对合理性认定分析框架与方法作出相应确认、调整，以更好地实现制度规范功能。建构以信息“上云”行为类型化为基础的合理性分析架构，兼具司法与产业层面价值。司法层面，该分析架构的设计遵循了保密措施的设定逻辑以及合理性的内涵要求，为法院多层次、多向度考察商业秘密权人采取保密措施的主观意图与客观行为，防止陷入简单的是非判断，提供了可行的路径参考和方法遵循，可一定程度纾解当前云计算环境下合理性认定的司法困境。产业层面，云计算产业发展直接关系到我国信息化发展水平的提升与数字经济新动能的激发。虽然近年来，我国云计算产业市场规模增速保持强劲增长态势，但是企业“上云率”广度与深度不够是制约我国云计算产业发展的瓶颈，而问题背后的原因主要是我国云计算技术产品供给不足，且企业对于信息“上云”安全与保密的隐忧。建构以类型化区分为基础的合理性分析架构，一方面，利于化解当前商业秘密保护的法律障碍，为企业“上云”提供相对稳定的行为预期，一定程度打消“上云”信息不受商业秘密保护的顾虑；另一方面，利于推动云服务提供商适应用户信息存储处理的个性化、差异化需求，设计开发更加多元的云产品和服务，丰富云计算技术产品市场。当然，为更好地平衡权利人、云服务提供商与社会公众之间的利益，促进云服务提供商与权利人之间的相互合作，合理性认定分析框架中的考量因素以及相应内容的设定，还应经过司法实践的不断校验、打磨与调教，只有这样才能实现商业秘密保护中的多重制度目标。

Reasonableness Identification of Trade Secret Confidentiality Measures in Cloud Computing Environment

Nie Xin

(*Intellectual Property School, Nanjing University of Science and Technology, Jiangsu Nanjing* 210094, *China*)

Summary: Cloud computing has become an inevitable choice for the digital transformation of enterprises. The emergence and application of cloud computing as information storage and processing technology complicate the reasonableness identification of trade secret confidentiality

①Elizabeth A. Rowe. Contributory Negligence, Technology and Trade Secrets, George Mason Law Review, 17, 2009, p. 29.

②北京市朝阳区人民法院〔2017〕京民初第68514号民事判决书。

measures. First, the partial transfer of the management right of trade secret information makes cloud service providers enter the view of identification. Second, the retention of the right of access to the information content of "uploading to the cloud" by cloud service providers may lead to the risk of expanding the scope of confidential information to be known indefinitely. Third, the express exclusion of confidentiality responsibility by cloud service providers constitutes an obstacle to the reasonableness identification of confidentiality measures. The traditional framework and method of reasonableness identification need to be reshaped. Based on the logic of property disclosure of confidentiality measures and the relativity and economic connotation of reasonableness to prevent overprotection, combined with promoting the development of cloud computing industry, following the principle of net neutrality and considering the factors of examining the meaning of the right holder's confidentiality, behavior of uploading information to the cloud should be divided into information transfer or content disclosure in order to determine the reasonableness of trade secret confidentiality measures in cloud computing environment, and a three-step analysis method should be constructed. The first step is to determine that the type of information "uploading to the cloud" is information transfer or content disclosure based on the subjective and reasonable expectation of the right holder, the environment setting of cloud service products, and the actual information being known. If the behavior of "uploading to the cloud" is judged as information transfer, it means that the right holder has not shared and disclosed confidential information with cloud service providers, and the reasonableness identification directly enters the third step. If the behavior of information "uploading to the cloud" is identified as content disclosure, the reasonableness identification should enter the second step. The second step is the analysis of whether cloud service providers bear the confidentiality obligation, which mainly investigates whether cloud service providers bear the express or implied confidentiality obligation to the right holder. The third step is the analysis of the confidentiality measures taken by the right holder, which mainly focuses on the analysis of the enterprise type and industrial characteristics of the right holder, whether the trade secret information is defined and managed differently, whether appropriate confidentiality measures are taken according to the characteristics and value of trade secret information, and whether systematic risk assessment and prevention and control measures are taken.

Key words: cloud computing; confidentiality measures; reasonableness; disclosure

（责任编辑：倪建文）